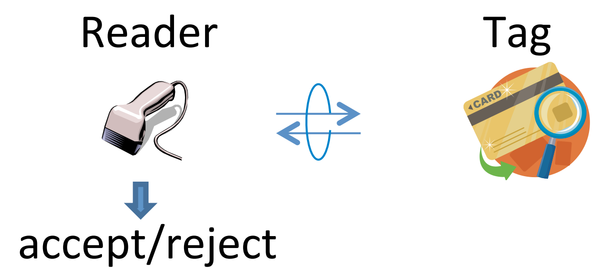
A Provably Secure Offline RFID Yoking-Proof Protocol with Anonymity

Daisuke Moriyama

NICT

Cryptographic Protocols Target on RFID tag

- RFID authentication protocol



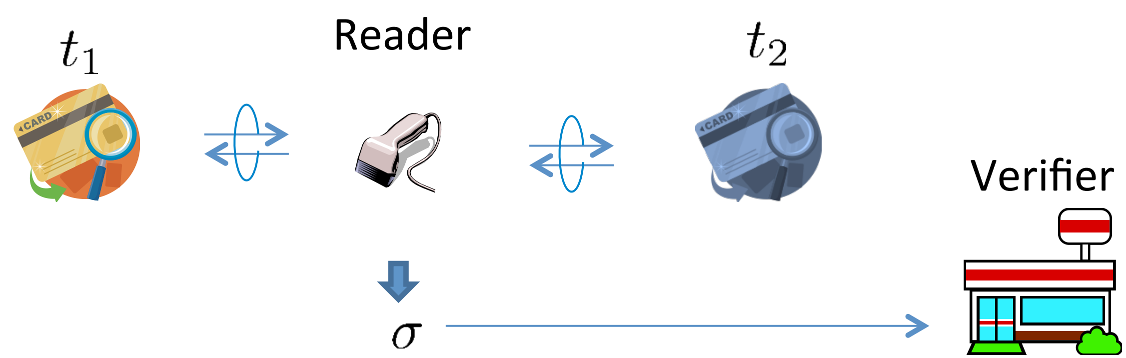
There are many results…

- RFID ownership transfer protocol

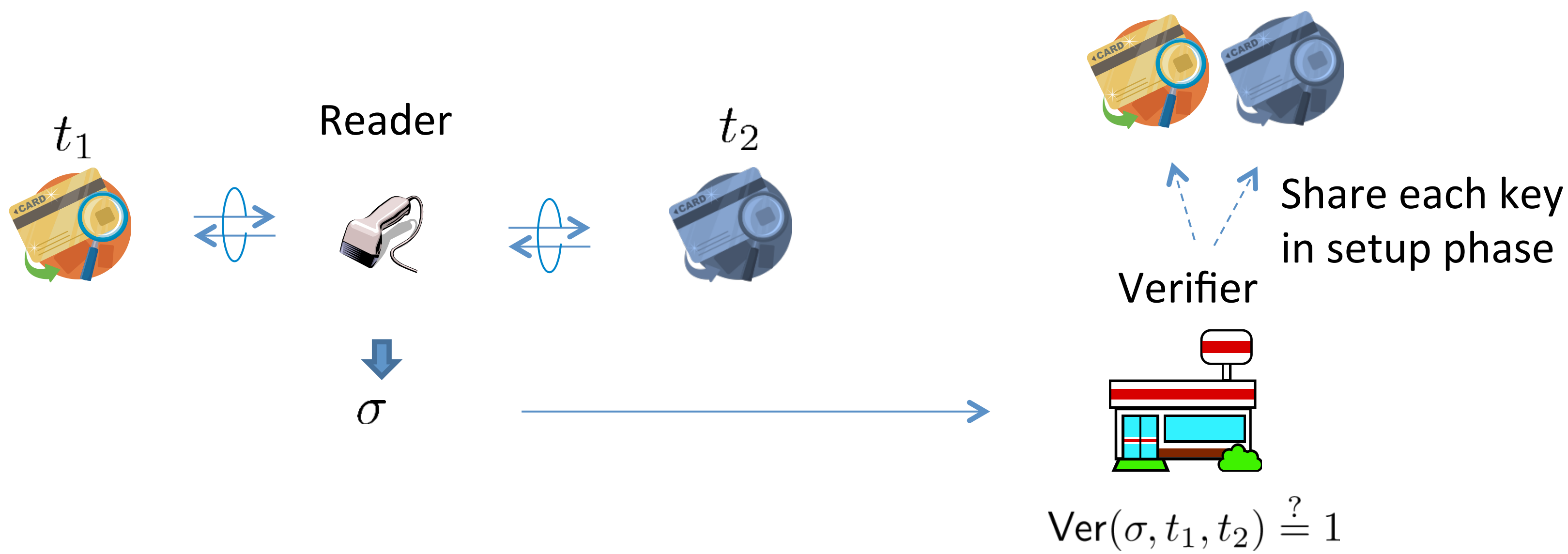
I proposed a provably secure protocol
at LightSec 2013

- RFID yoking/grouping proof protocol

This talk



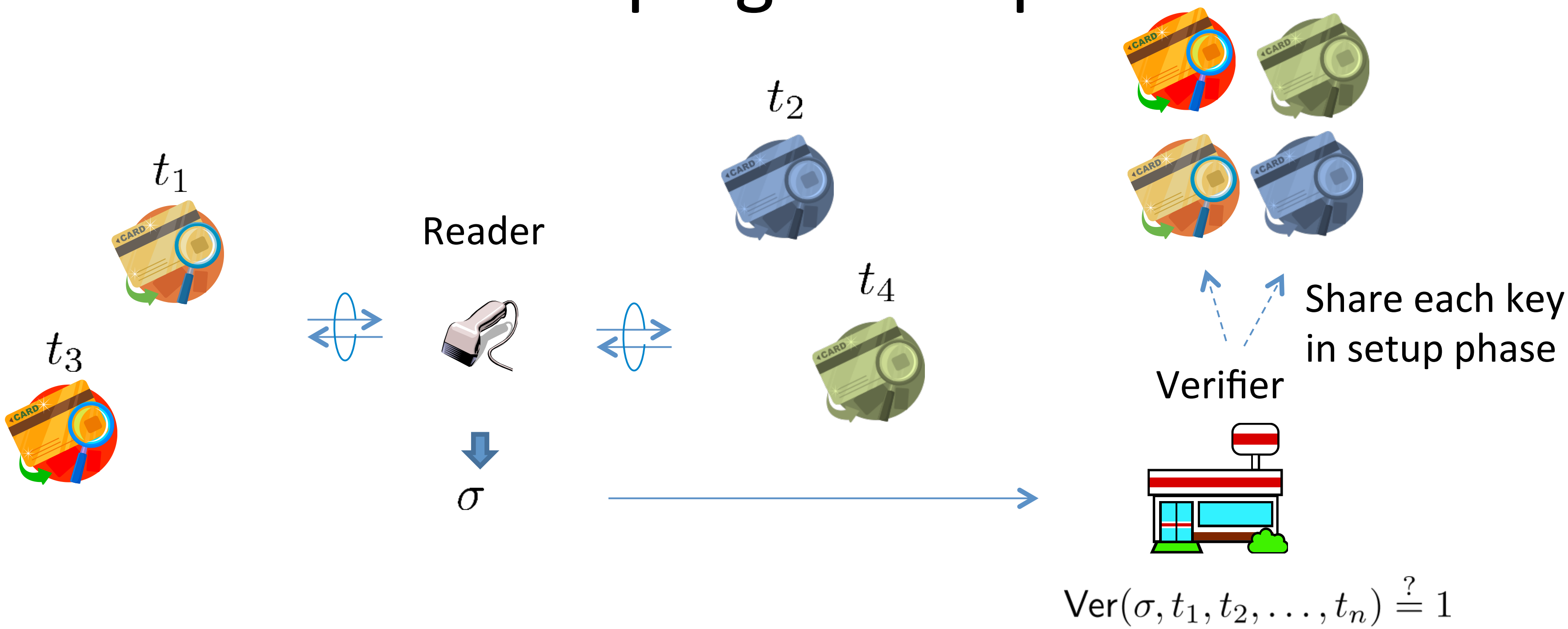
RFID Yoking-Proof protocol



- During a session, a reader communicates with two RFID tags
- Tags generate a "proof", which a (specific) verifier can check these tags were communicated with the reader in one session.

Juels, A.:
"Yoking-Proofs" for RFID Tags (PerSec 2004)

RFID Grouping-Proof protocol



- During a session, a reader communicates with multiple RFID tags
- Tags generate a "proof", which a (specific) verifier can check these tags were communicated with the reader in one session.

Saito, J., Sakurai, K.:
Grouping proof for RFID tags (AINA 2005)

Summary of the existing proposals and attack reports

Juels (PerSec2004) -> Saito,Sakurai (AINA 2005)

Bolotnyy,Robins (Mobiquitous2006) -> I could Attack

Saito,Sakurai (AINA2005) -> Pamamithu (SecPerU2006)

Pamamithu (SecPerU2006) -> Peris et al. (SecPerU2007)

Burmester et al. (CARDIS2008) -> Peris et al. (JNCA2011)

Chien,Liu (NSWCTC2009) -> Peris et al. (JNCA2011)

Huang,Ku (JoMS2009) -> Peris et al. (JNCA2011)

Duc,Kim(ePrint2009) -> I could attack

Peris et al. (JNCA2011) -> Bagheri,Safkhani (ePrint2013/453)

Batina et al. (JoPUC2012) -> Hermans,Peeters (RFIDSec2012)

Hermans,Peeters (RFIDSec2012) -> I could attack

Unfortunately, the existing protocols can be attacked!!!

Reason 1: No provable security

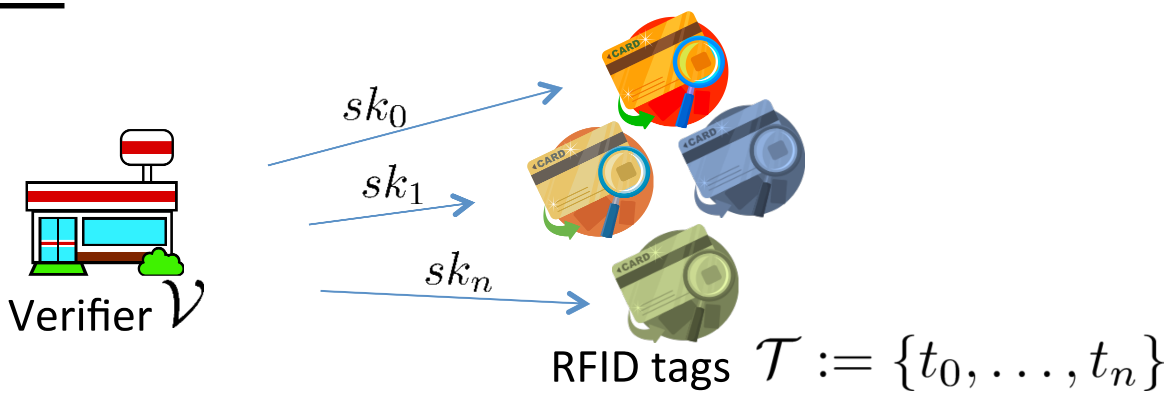
Reason 2: No definition for sufficient "security"

Propose a security model to achieve strong security is the first task

Security Model against Yoking-proof Protocols

Execution model

Setup Phase:



Yoking-Proof Generation Phase:

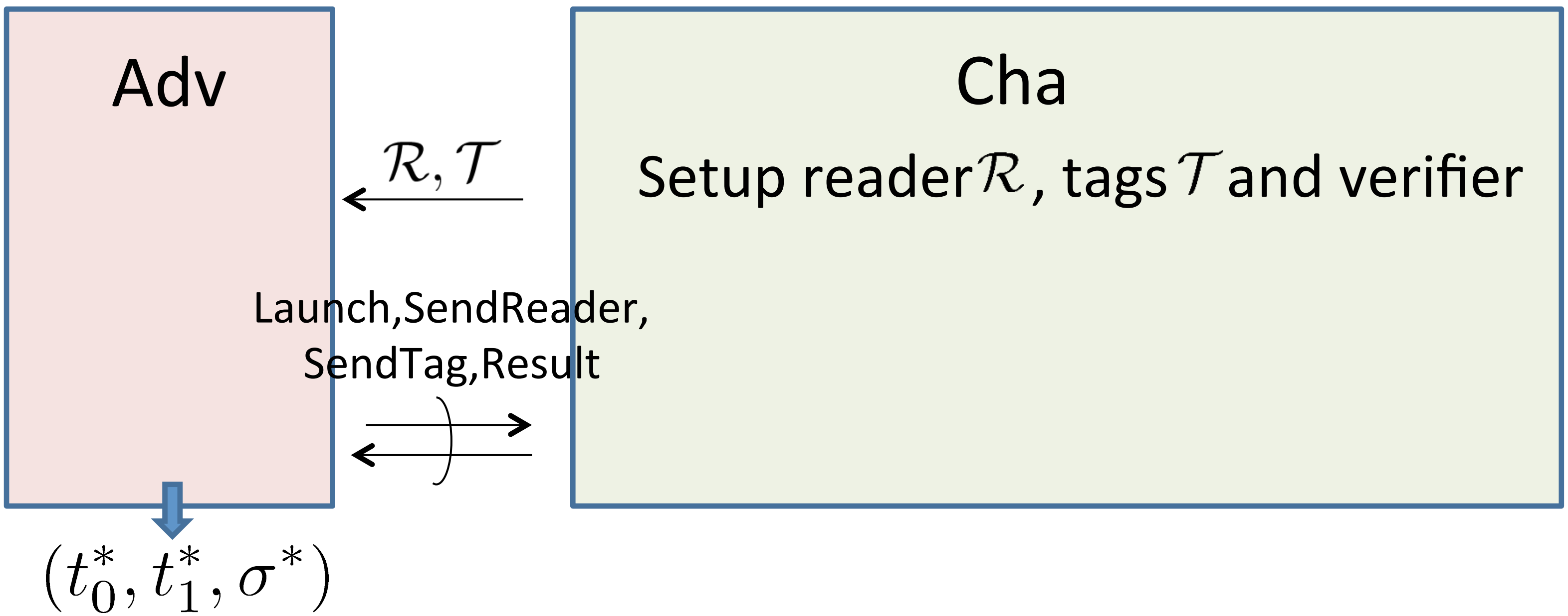
Two tags do not have direct communication but interaction via a reader

Verification Phase:

$$\mathsf{Ver}(sk, \mathcal{T}, \sigma) \stackrel{?}{=} 1$$

Verifier does not participate in the above phase and checks the validity of yoking-proof later in the offline case

Security against man-in-the-middle attack



Adv wins the security game if the verifier accepts σ^* on the condition that:

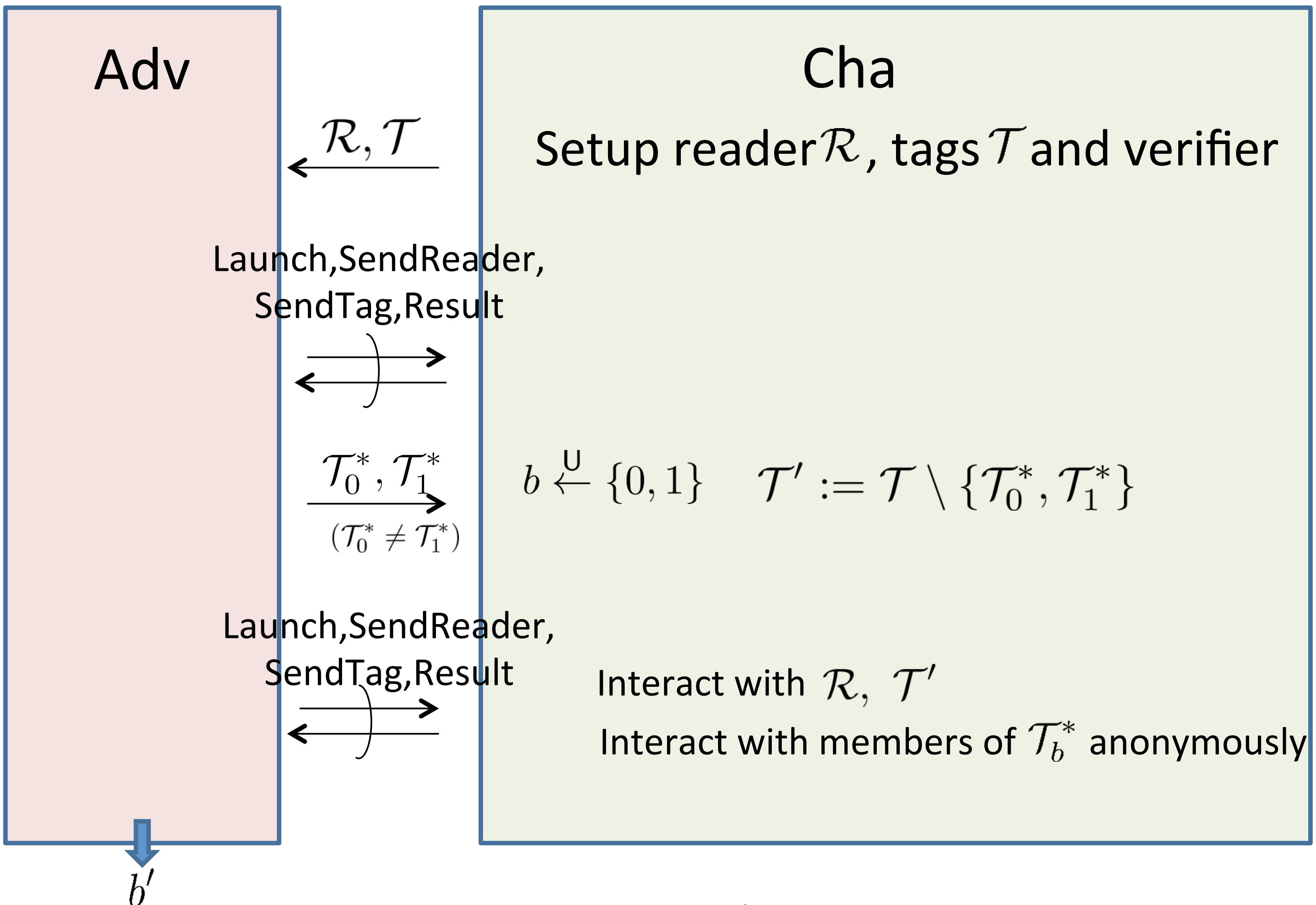
σ^* is not derived from a matching session between (t_0^*, t_1^*)

All communication messages between tags in a session is honestly transferred

$$t_0^* \xrightarrow[m]{} \mathcal{A} \xrightarrow[m']{} \mathcal{R} \xrightarrow[m']{} \mathcal{A} \xrightarrow[m]{} t_1^*$$

This is still honest communication !

Privacy (optional in yoking-proof)

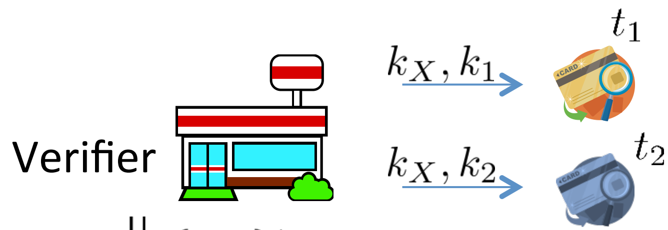


Adv wins the privacy game if $b' = b$

The Proposed Protocol

Anonymous RFID yoking-proof protocol

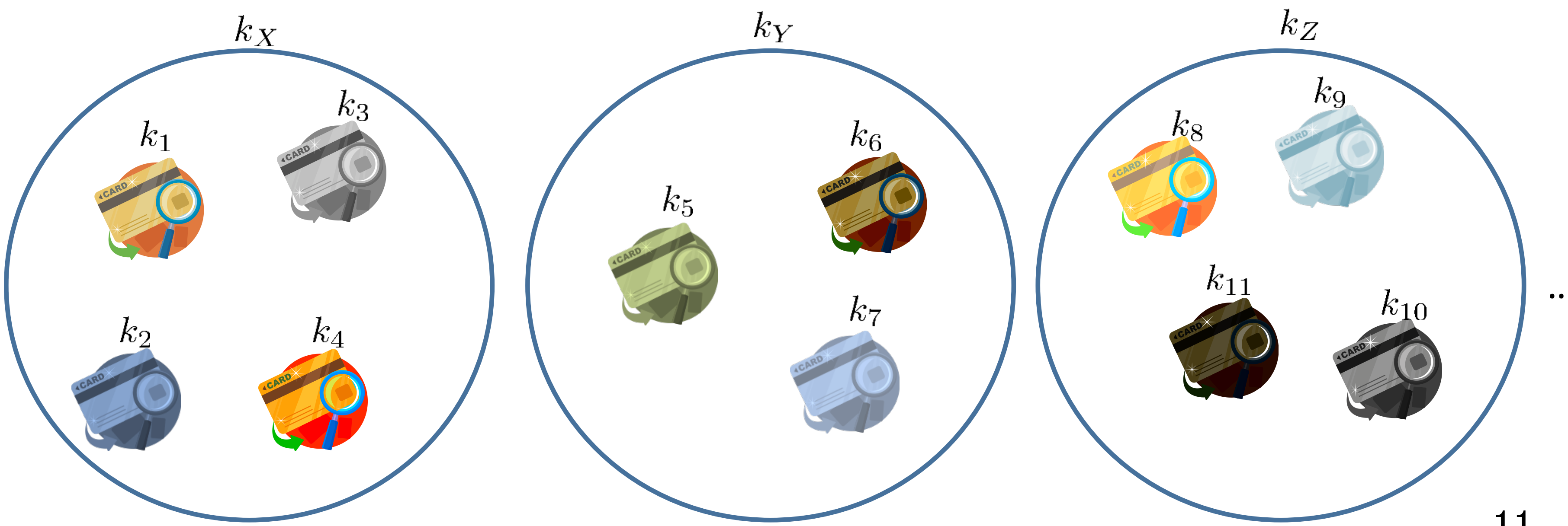
Setup Phase:



$k_X, k_1, k_2 \xleftarrow{U} \{0,1\}^*$

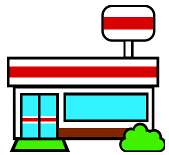
Hierarchical structure of the RFID tag:

- Consider groups of the tags
- One secret key is shared among the group, another key is unique for each tag



Anonymous RFID yoking-proof protocol

Setup Phase:

Verifier 

$k_X, k_1 \rightarrow$ t_1 

$k_X, k_2 \rightarrow$ t_2 

$k_X, k_1, k_2 \overset{\mathsf{U}}{\leftarrow} \{0,1\}^*$

Yoking-proof generation Phase:

ts : time stamp

$r \overset{\mathsf{U}}{\leftarrow} \{0,1\}^k$

$\xleftarrow{\text{ts}, r}$

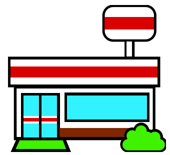
$r_1 \overset{\mathsf{U}}{\leftarrow} \{0,1\}^k$

$u_1 := \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1))$

$\xrightarrow{r, r_1, u_1}$

Anonymous RFID yoking-proof protocol

Setup Phase:

Verifier 

$k_X, k_1, k_2 \overset{U}{\leftarrow} \{0,1\}^*$

t_1  $\xrightarrow{k_X, k_1}$

t_2  $\xrightarrow{k_X, k_2}$

Generation Phase:

ts : time stamp

$r \overset{U}{\leftarrow} \{0,1\}^k$

$\xleftarrow{\mathsf{ts}, r}$

$r_1 \overset{U}{\leftarrow} \{0,1\}^k$

$u_1 := \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1))$

$\xrightarrow{r, r_1, u_1}$

$\xrightarrow{\mathsf{ts}, r, r_1, u_1}$

Check whether the message is came from a group member

$\boxed{u_1 \overset{?}{=} \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1))}$

$r_2 \overset{U}{\leftarrow} \{0,1\}^k$

$u_2 := \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1, r_2))$

$v_2 := \mathsf{PRF}(k_2, (\mathsf{ts}, r, r_1, r_2))$

$\text{Else}, r_2, u_2, v_2 \overset{U}{\leftarrow} \{0,1\}^{3k}$

$\xleftarrow{r, r_2, u_2, v_2}$

Anonymous RFID yoking-proof protocol

Setup Phase:

Verifier

$k_X, k_1, k_2 \xleftarrow{\mathsf{U}} \{0,1\}^*$

$\xrightarrow{k_X, k_1}$ t_1

$\xrightarrow{k_X, k_2}$ t_2

Generation Phase:

ts : time stamp

$r \xleftarrow{\mathsf{U}} \{0,1\}^k$

$\xleftarrow{\mathsf{ts}, r}$

$r_1 \xleftarrow{\mathsf{U}} \{0,1\}^k$

$u_1 := \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1))$

$\xrightarrow{r, r_1, u_1}$ $\xrightarrow{\mathsf{ts}, r, r_1, u_1}$

$u_1 \stackrel{?}{=} \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1))$

$r_2 \xleftarrow{\mathsf{U}} \{0,1\}^k$

$u_2 := \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1, r_2))$

$v_2 := \mathsf{PRF}(k_2, (\mathsf{ts}, r, r_1, r_2))$

$\mathrm{Else}, r_2, u_2, v_2 \xleftarrow{\mathsf{U}} \{0,1\}^{3k}$

$\xleftarrow{r_1, r_2, u_2}$ $\xleftarrow{r, r_2, u_2, v_2}$

$\boxed{u_2 \stackrel{?}{=} \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1, r_2))}$

$v_1 := \mathsf{PRF}(k_1, (\mathsf{ts}, r, r_1, r_2))$

$\mathrm{Else}, v_1 \xleftarrow{\mathsf{U}} \{0,1\}^k$

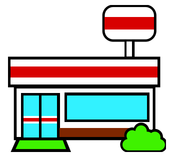
$\xrightarrow{r, v_1}$

$$\sigma := (\mathsf{ts}, r, r_1, r_2, u_2, v_1, v_2)$$

Check whether the message is came from a group member and the peer responds against r_1

Anonymous RFID yoking-proof protocol

Setup Phase:



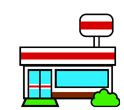
Verifier

t_1: $k_X, k_1 \rightarrow$

t_2: $k_X, k_2 \rightarrow$

$k_X, k_1, k_2 \overset{U}{\leftarrow} \{0,1\}^*$

Generation Phase:



ts : time stamp

$r \overset{U}{\leftarrow} \{0,1\}^k$

$\xleftarrow{\mathsf{ts}, r}$

$r_1 \overset{U}{\leftarrow} \{0,1\}^k$

$u_1 := \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1))$

$\xrightarrow{r, r_1, u_1}$ $\xrightarrow{\mathsf{ts}, r, r_1, u_1}$

$u_1 \overset{?}{=} \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1))$

$r_2 \overset{U}{\leftarrow} \{0,1\}^k$

$u_2 := \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1, r_2))$

$v_2 := \mathsf{PRF}(k_2, (\mathsf{ts}, r, r_1, r_2))$

$\text{Else}, r_2, u_2, v_2 \overset{U}{\leftarrow} \{0,1\}^{3k}$

$\xleftarrow{r_1, r_2, u_2}$ $\xleftarrow{r, r_2, u_2, v_2}$

$u_2 \overset{?}{=} \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1, r_2))$

$v_1 := \mathsf{PRF}(k_1, (\mathsf{ts}, r, r_1, r_2))$

$\text{Else}, v_1 \overset{U}{\leftarrow} \{0,1\}^k$

$\xrightarrow{r, v_1}$

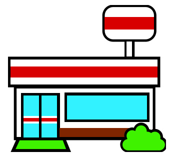
$\sigma := (\mathsf{ts}, r, r_1, r_2, u_2, v_1, v_2)$

$$\left\{\begin{array}{l} u_2 \overset{?}{=} \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1, r_2)) \\ v_1 \overset{?}{=} \mathsf{PRF}(k_1, (\mathsf{ts}, r, r_1, r_2)) \\ v_2 \overset{?}{=} \mathsf{PRF}(k_2, (\mathsf{ts}, r, r_1, r_2)) \end{array}\right.$$

All outputs from PRFs are bound by same input

Anonymous RFID yoking-proof protocol

Setup Phase:

Verifier 

$k_X, k_1 \rightarrow$ t_1 

$k_X, k_2 \rightarrow$ t_2 

$k_X, k_1, k_2 \xleftarrow{\mathsf{U}} \{0,1\}^*$

Ge

Verifier needs to execute an exhaustive search for privacy
(similar to the canonical RFID authentication protocol)

But the hierarchy of the tag enables faster verification

1. Find a valid group secret key k_X which satisfies $u_2 \stackrel{?}{=} \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1, r_2))$
2. Find two tags by checking (v_1, v_2)

$u_2 \stackrel{?}{=} \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1, r_2))$

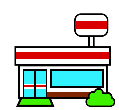
$v_1 := \mathsf{PRF}(k_1, (\mathsf{ts}, r, r_1, r_2))$

$\text{Else}, v_1 \xleftarrow{\mathsf{U}} \{0,1\}^k$ $\xrightarrow{r, v_1}$

$, r, r_1, r_2))$

$\text{Else}, r_2, \ldots \}^{3k}$

$\sigma := (\mathsf{ts}, r, r_1, r_2, u_2, v_1, v_2)$



$$\begin{cases} u_2 \stackrel{?}{=} \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1, r_2)) \\ v_1 \stackrel{?}{=} \mathsf{PRF}(k_1, (\mathsf{ts}, r, r_1, r_2)) \\ v_2 \stackrel{?}{=} \mathsf{PRF}(k_2, (\mathsf{ts}, r, r_1, r_2)) \end{cases}$$

Security Proof: security against man-in-the-middle attack

Assume $\sigma^* := (\mathsf{ts}^*, r^*, r_1^*, r_2^*, u_2^*, v_1^*, v_2^*)$ is the final output of the adversary

v_1^* is accepted on the condition that t_1 does not output it

$\longrightarrow$ The security of $\mathsf{PRF}(k_1, \cdot)$ can be broken

v_2^* is accepted on the condition that t_2 does not output it

$\longrightarrow$ The security of $\mathsf{PRF}(k_2, \cdot)$ can be broken

(v_1^*, v_2^*) is reused from a session

$\longrightarrow$ PRF is deterministic and the verifier accepts only if the remained tuple is also generated by t_1 and t_2

$\longrightarrow$ Man-in-the-middle attack is impossible

$u_2 := \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1, r_2))$

$v_2 := \mathsf{PRF}(k_2, (\mathsf{ts}, r, r_1, r_2))$

$\text{Else}, r_2, u_2, v_2 \xleftarrow{\mathsf{U}} \{0,1\}^{3k}$

$\xleftarrow{r, r_2, u_2, v_2}$

$\xleftarrow{r_1, r_2, u_2}$

$u_2 \stackrel{?}{=} \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1, r_2))$

$v_1 := \mathsf{PRF}(k_1, (\mathsf{ts}, r, r_1, r_2))$

$\text{Else}, v_1 \xleftarrow{\mathsf{U}} \{0,1\}^k$

$\xrightarrow{r, v_1}$

$$\sigma := (\mathsf{ts}, r, r_1, r_2, u_2, v_1, v_2)$$

$$\left\{ \begin{array}{l} u_2 \stackrel{?}{=} \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1, r_2)) \\ v_1 \stackrel{?}{=} \mathsf{PRF}(k_1, (\mathsf{ts}, r, r_1, r_2)) \\ v_2 \stackrel{?}{=} \mathsf{PRF}(k_2, (\mathsf{ts}, r, r_1, r_2)) \end{array} \right.$$

Security proof: privacy (Game 0)

Generation Phase:

$\xleftarrow{\ \mathsf{ts}, r\ }$

$r_1 \overset{\mathsf{U}}{\leftarrow} \{0,1\}^k$

$u_1 := \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1))$

$\xrightarrow{\ r, r_1, u_1\ }$ $\xrightarrow{\ \mathsf{ts}, r, r_1, u_1\ }$

$u_1 \overset{?}{=} \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1))$

$r_2 \overset{\mathsf{U}}{\leftarrow} \{0,1\}^k$

$u_2 := \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1, r_2))$

$v_2 := \mathsf{PRF}(k_2, (\mathsf{ts}, r, r_1, r_2))$

$\text{Else}, r_2, u_2, v_2 \overset{\mathsf{U}}{\leftarrow} \{0,1\}^{3k}$

$\xleftarrow{\ r_1, r_2, u_2\ }$ $\xleftarrow{\ r, r_2, u_2, v_2\ }$

$u_2 \overset{?}{=} \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1, r_2))$

$v_1 := \mathsf{PRF}(k_1, (\mathsf{ts}, r, r_1, r_2))$

$\text{Else}, v_1 \overset{\mathsf{U}}{\leftarrow} \{0,1\}^k$

$\xrightarrow{\ r, v_1\ }$

$$\sigma := (\mathsf{ts}, r, r_1, r_2, u_2, v_1, v_2)$$

$$\left\{ \begin{array}{l} u_2 \overset{?}{=} \mathsf{PRF}(k_X, (\mathsf{ts}, r, r_1, r_2)) \\ v_1 \overset{?}{=} \mathsf{PRF}(k_1, (\mathsf{ts}, r, r_1, r_2)) \\ v_2 \overset{?}{=} \mathsf{PRF}(k_2, (\mathsf{ts}, r, r_1, r_2)) \end{array} \right.$$

Security proof: privacy (Game 1-j)

- Replace $\mathsf{PRF}(k_X, \cdot)$ (PRF using a j-th group secret key) to a truly random function

Generation Phase:

ts, r ←

$r_1 \xleftarrow{U} \{0,1\}^k$
$u_1 \xleftarrow{U} \{0,1\}^k$

r, r_1, u_1 →

ts, r, r_1, u_1 →

check u_1

$r_2 \xleftarrow{U} \{0,1\}^k$
$u_2 \xleftarrow{U} \{0,1\}^k$
$v_2 := \mathsf{PRF}(k_2, (\mathsf{ts}, r, r_1, r_2))$
$\mathrm{Else}, r_2, u_2, v_2 \xleftarrow{U} \{0,1\}^{3k}$

r_1, r_2, u_2 ←

r, r_2, u_2, v_2 ←

check u_2

$v_1 := \mathsf{PRF}(k_1, (\mathsf{ts}, r, r_1, r_2))$
$\mathrm{Else}, v_1 \xleftarrow{U} \{0,1\}^k$

r, v_1 →

$$\sigma := (\mathsf{ts}, r, r_1, r_2, u_2, v_1, v_2)$$

check u_2

$$\left\{ \begin{array}{l} v_1 \stackrel{?}{=} \mathsf{PRF}(k_1, (\mathsf{ts}, r, r_1, r_2)) \\ v_2 \stackrel{?}{=} \mathsf{PRF}(k_2, (\mathsf{ts}, r, r_1, r_2)) \end{array} \right.$$

Security proof: privacy (Game 2-j)

- Replace $\mathsf{PRF}(k_X, \cdot)$ (PRF using a j-th group secret key) to a truly random function
- Replace $\mathsf{PRF}(k_j, \cdot)$ (PRF using a j-th individual secret key) to a truly random function

Generation Phase:



ts, r

$r_1 \xleftarrow{\mathsf{U}} \{0,1\}^k$

$u_1 \xleftarrow{\mathsf{U}} \{0,1\}^k$

r, r_1, u_1

ts, r, r_1, u_1

check u_1

$r_2 \xleftarrow{\mathsf{U}} \{0,1\}^k$

$u_2 \xleftarrow{\mathsf{U}} \{0,1\}^k$

$v_2 := \mathsf{PRF}(k_2, (\mathsf{ts}, r, r_1, r_2))$

$\mathrm{Else}, r_2, u_2, v_2 \xleftarrow{\mathsf{U}} \{0,1\}^{3k}$

r_1, r_2, u_2

r, r_2, u_2, v_2

check u_2

$v_1 \xleftarrow{\mathsf{U}} \{0,1\}^k$

r, v_1

$\sigma := (\mathsf{ts}, r, r_1, r_2, u_2, v_1, v_2)$

check u_2

check v_1

$v_2 \stackrel{?}{=} \mathsf{PRF}(k_2, (\mathsf{ts}, r, r_1, r_2))$

Security proof: privacy (Game 2-j)

After the game transformation is finished, communication messages include no information about the identity of the RFID tag

→ There is no opportunity for the adversary to violate privacy game

nction

nction

Generation Phase:

ts, r ←

$r_1 \overset{U}{\leftarrow} \{0,1\}^k$

$u_1 \overset{U}{\leftarrow} \{0,1\}^k$

r, r_1, u_1 →

ts, r, r_1, u_1 →

check u_1

$r_2 \overset{U}{\leftarrow} \{0,1\}^k$

$u_2 \overset{U}{\leftarrow} \{0,1\}^k$

$v_2 \overset{U}{\leftarrow} \{0,1\}^k$

Else, $r_2, u_2, v_2 \overset{U}{\leftarrow} \{0,1\}^{3k}$

r, r_2, u_2, v_2 ←

r_1, r_2, u_2 ←

check u_2

$v_1 \overset{U}{\leftarrow} \{0,1\}^k$

r, v_1 →

$\sigma :=$ (ts, $r, r_1, r_2, u_2, v_1, v_2$)

check u_2

check v_1

check v_2

Open problems

1. Extend to the grouping-proof protocol
    - Who checks whether all group members are interacted?

2. Privacy against tag corruption
    - Shared key mechanism in the same group is useless

3. Evaluation with implementation
    - No implementation result

Conclusion

- There is no secure RFID yoking/grouping-proof protocol
- We formalize a strong security model for RFID yoking-proof
- We propose the first RFID yoking-proof protocol provably secure against man-in-the-middle attack
- Our protocol also satisfies anonymity such that no party except the verifier can learn the identity of the RFID tag